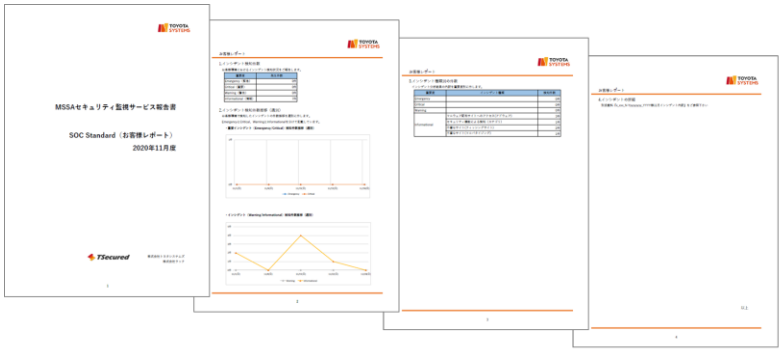
提供サービス内容

標準サービス	
ログの収集と分析	●分析対象機器より出力される、監視対象端末が外部（インターネット/イントラネット）と通信を行った際の通信記録をセキュリティ分析システムに集約し、複雑・巧妙化する高度なサイバー攻撃の動向、不正IPの履歴などさまざまな要因をもとに相関分析を行います。 ●分析対象機器から、セキュリティ分析システムに収集されたログを、セキュリティアナリストが分析します。 ●収集されたログの保管期間と過去ログ検索期間は3ヵ月 ※分析対象機器がトヨタシステムズ提供サービスの場合、お客様側での導入作業は不要です。 ※分析対象機器がお客様宅内の場合、ログ転送はお客様にてログ収集サーバまたはサービス対象機器へログ転送プログラムの導入が必要です。
インシデントの判定と通知	●インシデント発生時はセキュリティアナリストが以下の5段階に分類します。 ［Emergency（緊急）］［Critical（重要）］［Warning（警告）］［Informational（情報）］［False Positive（誤検知）］ ●セキュリティ監視・予防遮断は、２４時間３６５日（JST）でご提供いたします。 ●重要セキュリティインシデント（Emergency、Critical）の通知・緊急遮断・問い合わせ対応は、８時－１７時３６５日（JST）電話およびメールでご提供します。 ●重要度の低いセキュリティインシデント（Warning、Information）は、レポートにてお知らせします。
セキュリティ情報の提供	●独自入手情報および公開情報から収集した最新の脅威情報を、セキュリティアナリストが独自に精査。更新への追従を行い、セキュリティ分析ルールを随時更新 ●月次レポートをお客様に提出

月次レポート（サンプル）

- ご加入のお客様全体の傾向
- お客様環境で発生した攻撃内容
- セキュリティ関連トピックス



※イメージ

TOYOTA SYSTEMS
株式会社トヨタシステムズ
TEL：050-3142-7889　Mail：helpdesk01@tns.toyotasystems.com
URL：https://www.toyotasystems.com

2022年第1版